AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. (Currently Amended) A method for detecting unauthorized intrusion in a network system, comprising the steps of:

receiving packet level activity information from the network;

collecting continuous and sequential samples of ~~sorted~~ port specific ~~activity~~ information from the received packet level activity information for each IP/user wherein many packets are accumulated in any one sampling interval for each IP/user;

recognizing predefined ~~converting~~ and specific human behavior elements associated with normal and malicious activity from the accumulated packets in a sample of ~~sorted~~ packet level activity and indicating the presence of absence of these predefined ~~into~~ ~~human~~ behaviors and activities for each IP/user~~, including assigning a binary representation~~ with a designation of [(]1 (=present) or [,]0 (=absent) ~~to each human behavior and activity~~; and

processing in real-time the presence or absence of identified behavior elements for each IP/user occurring within a set sampling interval with a pre-trained neural network behavior assessment pattern classifier into behavior assessment measures of the amount of "expertise" and "deception" present for each IP/user for a given sampling interval as measures of underlying malicious or non-malicious intent, the trained pattern classifier converting any combination of the predefined behavior elements present for an IP/user for any sampling interval to non-

signature and non-anomaly based, pattern classifier determined, assessments of the level of expertise and deception represented by the behavior elements present for that IP/User's sampling interval, and wherein if operator determined thresholds for degree of expertise and deception are exceeded, a network connection blocking action is activated automatically ~~converting the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user in order to generate an assessment, wherein the assessment is made for every possible combination of behaviors and activities whether or not such combinations of behaviors and activities have been previously encountered and executing at least one of a network connection blocking action or passive gathering of tracked intent information for any given IP/user based upon the assessment indicating that the monitored expertise and deception exceed intent thresholds that indicate misuse network activity~~.

2. (Cancelled)

3. (Currently Amended) The method according to claim 1, wherein the step of generating an assessment includes associating ~~the~~ a binary rating with an assessment based upon predetermined behavioral criteria.

4. (Currently Amended) The method according to claim 3, wherein the step of ~~generating an assessment~~ processing includes mapping the assessment on at least one two-dimensional grid.

5. (Cancelled)

6. (Currently Amended) The method according to claim 1, wherein the step of processing ~~generating an assessment~~ includes generating a profile of the IP/user based upon the monitored behavioral measures.

7. (Currently Amended) The method according to claim 1, wherein the step of processing ~~generating an assessment~~ is carried out utilizing a back propagation network.

8. (Original) The method according to claim 7 wherein the back propagation network includes psychological assessment information.

9. (Previously Presented) The method according to claim 1, wherein the assessment is one of high deception/high expertise, high deception/low expertise, low deception/high expertise and low deception/low expertise.

10. (Previously Presented) The method according to claim 1, wherein the blocking action includes sending a blocking command to a firewall for blocking further network access if high deception and/or high expertise exceeds the threshold.

11. (Currently Amended) The method according to claim 1, wherein the ~~tracking action~~ step of collecting includes storing activity information in a tracking module.

12. (Currently Amended) A system for preventing unauthorized intrusion in a network system, comprising:

a traffic sorter that receives a copy of the network activity and sorts all activities by IP/User for the purpose collecting continuous and sequential samples of each IP/user's activities/behaviors, wherein many packets are accumulated in any one sampling interval for each IP/user;

an activity monitor operatively coupled to the traffic sorter for sequentially monitoring converted human intent behaviors and activities by IP/users;

an inter-port fusion module operatively coupled to the activity monitor that fuses assessments from one or more assessment engines that monitor behavior measures by IP/User and

an outcome director operatively coupled to the inter-port fusion monitor that determines whether to block or track IP/users on a specific IP/User basis based upon assessed behavioral measures of intent, wherein the assessed behavioral measure of intent are made for every possible combination of behaviors and activities whether or not such combinations of behaviors and activities have been previously encountered and, wherein the activity monitor includes at least one dedicated behavior monitor, wherein the at least one dedicated behavior monitor includes an activity /behavior analysis module, an activity translator module and an assessment module and wherein the assessment module includes a trained back propagation network, wherein the back propagation network provides combined expertise and deception ratings for each single monitored behavior.

13-15. (Cancelled)

16. (Previously Presented) The system according to claim 12, wherein the back propagation network includes psychological assessment information.

17. (Previously Presented) The system according to claim 12, wherein the traffic sorter receives packet level activity information from the network and sorts the port specific activity information from the network into IP/Users.

18. (Previously Presented) The system according to claim 12, wherein the activity monitor monitors the port and across-port specific activity information.

19. (Previously Presented) The system according to claim 12, wherein the activity translator module assigns a binary rating based upon presence (1) or absence (0) of at least one activity/behavior detected by the packet level analysis module.

20. (Previously Presented) The system according to claim 19, wherein the assessment module generates an assessment of levels of expertise and deception present in any sample of an IP/User's overall activities/behaviors for a collection interval.

21. (Previously Presented) The system according to claim 19, wherein the assessment module maps the assessment result utilizing at least one of a two dimensional grid or X dimensional grid for optional real-time viewing of a user's intent for each sequential collection interval.

22. (Original) The system according to claim 20, wherein an outcome director initiates at least one of a blocking command or a tracking command based upon the assessment result.

23. (Original) The system according to claim 22, wherein the blocking command is directed to a system firewall.

24. (Previously Presented) The system according to claim 23 in which a blocking command results in the loss of the connection between an IP/User and the network and the storage of all relevant session data up to the point of forced loss of the IP/User's connection to the network,

25. (Original) The system according to claim 22, wherein the tracking command is directed to a tracking module.

26. (Original) The system according to claim 24, wherein the tracking module includes a tracking database for storing activity information that may be used to provide evidence of an intruder's harmful intent activities and at least one intent assessment during a session.

27. (Original) The system according to claim 26, wherein the tracking database includes neural network assessment and associated information for the intruder that is at least one of tracked or blocked.

28. (Original) The system according to claim 27, wherein the tracking database includes a comparison module for comparing the neural network assessment and associated information against a second assessment based upon a second network intrusion.

29. (Original) The system according to claim 28, wherein at least one of a blocking or tracking action is executed based upon an output from the comparison module.

30. (Cancelled)

31. (Currently Amended) A computer program product, comprising:

a computer usable medium having computer readable code embodied therein for preventing unauthorized intrusion into a computer network, the computer program product comprising:

computer readable program code configured to cause the computer to continuously receive sequential samples of port specific information from each IP/user wherein many packets are accumulated in a sampling interval for each IP/user ~~process a copy of network activity in real-time to collect sequential samples of sorted port specific and non-port specific activity information for each IP/user from packet level activity information received by the computer network~~;

computer readable program code configured to cause the computer to recognize predefined and specific human behavior elements associated with normal and malicious activity from the accumulated packets in a sample of packet level activity and indicating the presence of absence of these predefined behaviors and activities for each IP/user with a designation of 1 (=present) or 0 (=absent) ~~convert the packet level activity into human behaviors and activities for each IP/user and convert the sorted IP/user behavioral activities into behavioral measures of expertise and deception as measures of underlying intent for each IP/user in order to generate an assessment, wherein the assessment is made for every possible combination of behaviors and activities whether or not such combinations of behaviors and activities have been previously encountered~~; and

computer readable program code configured to cause the computer to process in real-time the presence or absence of identified behavior elements for each IP/user occurring within a set sampling interval with a pre-trained neural network behavior assessment pattern classifier into behavior assessment measures of the amount of "expertise" and "deception" present for each IP/user for a given sampling interval as measures of underlying malicious or non-malicious intent, the trained pattern classifier converting any combination of the predefined behavior elements present for an IP/user for any sampling interval to non-signature and non-anomaly based, pattern classifier determined, assessments of the level of expertise and deception represented by the behavior elements present for that IP/User's sampling interval, and wherein if operator determined thresholds for degree of expertise and deception are exceeded, a network connection blocking action is activated automatically ~~execute at least one of a network connection blocking action or passive gathering of tracked intent information for any given IP/user based upon the assessment indicating that monitored expertise and deception exceed intent thresholds that indicate misuse network activity~~.

32. (Currently Amended) The method according to claim 1, wherein the step of receiving ~~the port and non-port specific activity/behavior information~~ includes creating a copy of the network activity sorted by users.

33. (Previously Presented) The method according to claim 1, further including the step of sorting non-port specific activity information from the received packet level activity information by IP/user; and converting the non-port specific activity information to human behavioral measures of intent.